UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/851,956	05/09/2001	David Carroll Challener	RPS9 2001 0022	4042

45211 7590 02/03/2009
Robert A. Voigt, Jr.
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3692	

MAIL DATE	DELIVERY MODE
02/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DAVID CARROLL CHALLENER

Appeal 2008-4043
Application 09/851,956
Technology Center 3600

Decided:[1] February 3, 2009

Before HUBERT C. LORIN, ANTON W. FETTING and BIBHU R. MOHANTY, *Administrative Patent Judges.*

LORIN, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

David C. Challener (Appellant) seeks our review under 35 U.S.C. § 134 of the Final Rejection of claims 1-27. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

SUMMARY OF DECISION

We REVERSE.[2]

THE INVENTION

The invention is directed to a method and system for obtaining a credit card online using the Trusted Computing Platform Alliance Specification. (Specification 3: 3-5.) To apply for a credit card, a customer sends an application, a public portion of a non-migratable storage key, a certificate from a Trusted Platform Module, and a certificate from a Certification Authority to a credit card company. (Specification 3: 7-12.) If the application is approved, the credit card company sends a public/private key pair and a certificate back to the customer. (Specification 3: 12-15.) The public/private key pair and the certificate are encrypted with the non-migratable storage key. *Id.* The customer will decrypt the public/private key pair and the third certificate and use the private key in the same manner as a physical credit card. (Specification 3: 15-20.)

Claim 1, reproduced below, is illustrative of the subject matter on appeal.

[2] Our decision will make reference to the Appellant's Appeal Brief ("App. Br.," filed Mar. 27, 2007) and Reply Brief ("Reply Br.," filed Oct. 19, 2007), and the Examiner's Answer ("Answer," mailed Aug. 21, 2007).

> 1. A method comprising the steps of:
>
> receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA);
>
> creating a public/private key pair and a third certificate in response to the receiving step; and
>
> sending the public/private key pair and the third certificate to the customer over the network.

THE REJECTIONS

The Examiner relies upon the following as evidence of unpatentability:

Trusted Computing Performance Alliance, (TCPA) TCPA Design Philosophies and Concepts 1-30 (Version 1.0, 2000). (Hereinafter "TCPA").

The following rejection is before us for review:

1. Claims 1-27 are rejected under 35 U.S.C. §103(a) as being unpatentable over TCPA.

ISSUES

The first issue before us is whether the Appellant has shown that the Examiner erred in rejecting claims 1-6, 16-20, and 25 under 35 U.S.C. § 103(a) as being unpatentable over TCPA. The issue turns on whether TCPA and the general knowledge in the art that credit card applications can be sent to credit card companies over a network would lead one of ordinary skill in the art to a method and system for a credit card company creating a public/private key pair in response to receiving a credit card application, an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a certification authority."

The second issue before us is whether the Appellant has shown that the Examiner erred in rejecting claims 7-15, 21-24, 26 and 27 under 35 U.S.C. § 103(a) as being unpatentable over TCPA. The issue turns on whether TCPA and the general knowledge in the art that credit card applications can be sent to credit card companies over a network would lead one of ordinary skill in the art to a method and system creating a TPM identity, creating a non-migratable key and transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company.

FINDINGS OF FACT

We find that the following enumerated findings of fact (FF) are supported by at least a preponderance of the evidence. *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988) (explaining the general evidentiary standard for proceedings before the Office).

Claim construction

1. Claim 1 recites a method comprising the step of "receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer

system used by the customer, and a second certificate acquired by the computer system from a Certification Authority."

2. Claim 1 also recites the step of "creating a public/private key pair and a third certificate in response to the receiving step."
3. Claim 7 recites a method comprising the step of "creating a TPM identity at a customer's computer system."
4. Claim 7 also recites "creating, at the customer's computer system, a non-migratable key."
5. Claim 7 recites "transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company."
6. Claim 16 recites a computer program comprising the program step of

> receiving from a customer over a network an application for a credit card authorization, a non-migratable key, a first certificate by a Trusted Platform Module (TPM) identity associated with a computer system used by the customer, and a second certificate acquired by the computer system from a Certification Authority (CA).

7. Claim 16 also recites "creating a public/private key pair and a third certificate in response to the receiving step."
8. Claim 21 recites a computer program product comprising the program steps of "creating a TPM identity."
9. Claim 21 recites "creating a non-migratable key."

10. Claim 21 also recites, “sending to the web site an application for a credit card authorization, the TPM identity, the first certificate, and the non-migratable key.”

11. Claim 25 recites “third software stored in memory in the customer computer for creating a non-migratable key.”

12. Claim 25 also recites “sixth software stored in memory in the customer computer for sending to the web site of the credit card company over the network the TPM identity, the first certificate, and the non-migratable key.”

13. Claim 25 also recites “the web site of the credit card company creating a public/private key pair and second certificate.”

14. Claim 26 recites a system comprising a CPU executing a code effective in “creating a TPM identity.”

15. Claim 26 recites “creating a non-migratable key.”

16. Claim 26 recites “transferring a credit card authorization application, said TPM identity, said non-migratable key, and said first certificate to said credit card application server.”

17. Claim 27 recites an apparatus comprising a TPM which creates a TPM identity.

18. Claim 27 also recites a CPU effective in “creating a non-migratable key and transferring said non-migratable key, said TPM identity, said first certificate, and a credit card authorization application to the credit card application server.”

The scope and content of the prior art

19. TCPA is an industry specification for a subsystem having a trusted platform module. (TCPA § 1.2 at 1.)

20. TCPA describes a Trusted Platform Module Entity (TPME) that vouches that a trusted platform module (TPM) is actually a TPM. (TCPA § 2.4.1.7 at 8.)

21. The TPME puts a private/public endorsement key in each trusted platform module and provides an endorsement credential for each trusted platform module. (TCPA § 2.4.1.7 at 8.)

22. TCPA describes that a certification authority verifies the public keys of another entity and provides a certificate. (TCPA § 2.4.2.1 at. 8.)

23. TCPA describes a method of obtaining a TPM identity. (TCPA § 2.5.1 at 9-10.)

24. To create an identity, the owner of the subsystem must make available information including: the endorsement credential, the platform credential, the conformance credential, and the public key of a privacy certification authority. (TCPA § 2.5.1 at 9.)

25. The information is used to provide credential from the certifying authority to the owner. (TCPA § 2.5.1 at 10.)

26. The TPM generates an identity (public) key and a signature (private) key for a new TPM identity. (TCPA § 2.5.1 at 10.)

27. The TPM identity is then associated with the credential provided by certifying authority. (TCPA § 2.5.1 at 10-11.)

28. TCPA states, "[t]he actual uses of a Subsystem are the choice of the manufacturer and outside the scope of this specification." (TCPA § 2.10 at 22.)

29. TCPA states that electronic business might benefit from the system. (TCPA § 1.4 at 4.)

30. The Specification states that currently a method of obtaining a credit card is to fill out an application at the credit card's website. (Specification 2:10-12.)

Any differences between the claimed subject matter and the prior art

31. TCPA does not describe a credit card company with a website or a server.

32. TCPA does not describe receiving an application for credit card authorization.

33. TCPA does not describe creating a public/private key pair and a third certificate in response to the receiving step.

34. TCPA does not describe sending the public/private key pair and the third certificate to the customer over the network.

The level of skill in the art

35. Neither the Examiner nor the Appellants has addressed the level of ordinary skill in the pertinent art of secure communications over data processing networks. We will therefore consider the cited prior art as representative of the level of ordinary skill in the art. *See Okajima v. Bourdeau,* 261 F.3d 1350, 1355 (Fed. Cir. 2001) ("[T]he absence of specific findings on the level of skill in the art does not give rise to reversible error 'where the prior art itself reflects an appropriate level and a need for testimony is not shown'") (Quoting *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 163 (Fed. Cir. 1985)).

Secondary considerations

36. There is no evidence on record of secondary considerations of non-obviousness for our consideration.

PRINCIPLES OF LAW

Claim Construction

During examination of a patent application, a pending claim is given the broadest reasonable construction consistent with the specification and should be read in light of the specification as it would be interpreted by one of ordinary skill in the art. *In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004).

> [W]e look to the specification to see if it provides a definition for claim terms, but otherwise apply a broad interpretation. As this court has discussed, this methodology produces claims with only justifiable breadth. *In re Yamamoto*, 740 F.2d 1569, 1571 (Fed. Cir. 1984). Further, as applicants may amend claims to narrow their scope, a broad construction during prosecution creates no unfairness to the applicant or patentee. *Am. Acad.*, 367 F.3d at 1364.

In re ICON Health and Fitness, Inc., 496 F.3d 1374, 1379 (Fed. Cir. 2007). Limitations appearing in the specification but not recited in the claim are not read into the claim. *E-Pass Techs., Inc. v. 3Com Corp.*, 343 F.3d 1364, 1369 (Fed. Cir. 2003).

Obviousness

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1734 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). *See also KSR*, 127 S. Ct. at 1734 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.") The Court in *Graham* further noted that evidence of secondary considerations "might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." 383 U.S. at 17-18.

ANALYSIS

The rejection of claims 1-6, 16-20, and 25 under § 103(a) as being unpatentable over TCPA.

The Appellant argues that the TCPA does not lead one of ordinary skill to the steps of 1) receiving a non-migratable key, a first certificate by a Trusted Platform Module identity and a second certificate acquired by the computer system from a Certifying Authority, 2) creating a public/private key pair and a third certificate in response to the receiving step, and 3) sending the public/private key pair and the third certificate to the customer over the network. (Br. 7-9.)

The Examiner found that TCPA described most of the limitations of the claims, including the steps of receiving a non-migratable key and creating a public/private key pair. (Answer 3.) However, the Examiner found that TCPA does not describe the step of receiving a credit card application, but that one of ordinary skill in the art knows that a credit card application from a customer can be received over a network. (Answer 4.)

The Examiner considered the claimed non-migratable key to be the private endorsement key of the public/private endorsement key pair. The Examiner stated, "... examiner submits that see page 9, section 2.5.1, the TPM contains a private endorsement key (a non-migratable key)." (Answer 7.) However, when referring to the step of creating a public/private key pair, the Examiner stated, "[t]he public key of that key pair is the TPM's 'public endorsement key.'" (Answer 7.) The Examiner pointed to TCPA's description of creating a TPM identity in section 2.5.1 to describe the steps of receiving the non-migratable key and sending the public private key pair. The Examiner concluded that combining TCPA with the knowledge that credit card applications can be received over a network renders the claims obvious under 35 U.S.C. § 103(a).

Independent claim 1 recites the steps of receiving from a customer a non-migratable key, a credit card application, a first certificate by a Trusted Platform Module identity and a second certificate from a Certifying Authority. (FF 1.) Claim 1 also recites creating a public/private key pair and a third certificate in response to the receiving step. (FF 2.) Independent claim 16 contains similar limitations. (FF 6-7.) Independent claim 25 recites a system including software stored in memory in the customer computer for creating a non-migratable key and sending the non-migratable key to a web site of a credit card company. (FF 11-12.) Claim 25 also recites the web site of the credit card company creating a public/private key pair. (FF 13.)

We find that the Examiner has not made a prima facie showing of obviousness. The Examiner seems to consider the private endorsement key to be both the claimed non-migratable key and the private portion of the claimed public/private key pair. (Answer 7.) However, the claims 1 and 16 recite that the public/private key pair is created *in response* to receiving the non-migratable key pair. Claim 25 recites that the system has software on the customer's computer for creating the non-migratable key while the credit card company's website is capable of creating the public/private key.

TCPA describes a trusted platform module entity, which causes the private/public endorsement key to be created for each of its trusted platform modules (TPM) it endorses. (FF 21.) TCPA does not describe the private/public endorsement key being created in response to receiving the non-migratable key pair, a credit card application, a first certificate or a second certificate as in claims 1 and 16. TCPA also does not describe the private/public endorsement key being created by either a customer or a credit card company's website as in claim 25.

Further, while TCPA does teach that the subsystem could be used in electronic business (FF 29), TCPA does not describe how the subsystem is used to interact with electronic businesses, such as credit card companies. TCPA states, "[t]he actual uses of a Subsystem are the choice of the manufacturer and are outside the scope of this specification." (TCPA § 2.10 at 22.) Further, the Examiner does not explain how TCPA and the general knowledge that credit card applications can be received over a network would lead one of ordinary skill in the art to the specific receiving, creating and sending steps of the claims.

We find that combining TCPA with the knowledge that credit card applications can be received over a network does not lead one of ordinary skill in the art to the claimed steps and system for creating a public/private key pair. A prima facie case of obviousness under 35 U.S.C. § 103(a) has therefore not been established, and we reverse the rejections of claims 1, 16 and 25 and their dependent claims 2-6 and 17-20.

The rejection of claims 7-15, 21-24, 26 and 27 under § 103(a) as being unpatentable over TCPA.

The Appellant argues that the Examiner has not effectively addressed claim 7 since the Examiner rejected claim 7 based on the same rational used from claims 1-6 after finding claims 1-6 contained similar limitations to claim 7. The Appellant states, "[t]here are no claim limitations in claim 7 that are similar to claims 1-6 such that the Examiner . . . has not presented a *prima facie* case of obviousness in rejecting claim 7, since the Examiner is relying upon incorrect, factual predicates in support of the rejection." (App. Br. 18-19.)

The Examiner found that claims 7, 21 and 26-27 contained similar limitations to claims 1-6 and therefore the same rationale applied to claim 1 applies to these claims. (Answer 9.) The Examiner's rationale as to claim 1 is discussed above.

Claim 7 recites the steps of, "creating a TPM identity," "creating at the customer's computer system, a non-migratable key" and "transferring a credit card authorization application, the TPM identity, the non-migratable key, and the first certificate from the customer's computer system to a second server supporting a credit card company." (FF 3-5.) Claims 26 and 27 includes similar limitations (FF 14-18). Claim 21 also includes a step of creating a TPM identity, creating a non-migratable key and sending to a website of a credit card company a credit card authorization, the TPM identity, the first certificate and the non-migratable key. (FF 8-10.)

In Section 2.5.1, TCPA describes a method of creating a TPM identity. In order to create the identity, the endorsement credential, the platform credential, the conformance credential and the public key of a privacy credential authority is sent to a privacy credential authority. (FF 24.) The privacy credential authority uses this information to provide the TPM with another credential. (FF 25.) The owner of the TPM then associates this new credential with the TPM identity. (FF 27.) The result is an identity (public) key, a signature (private) key and an associated certificate from a Certifying Authority for the TPM identity. (FF 26.)

Further, while TCPA does teach that the TPM subsystem could be used in electronic business (FF 29), TCPA does not describe how the subsystem is used to interact with electronic businesses, such as credit card companies. TCPA states, "[t]he actual uses of a Subsystem are the choice of the manufacturer and are outside the scope of this specification." (TCPA § 2.10 at 22.) Further, the Examiner does not explain how the method of creating a TPM identity described in TCPA and the general knowledge that credit card applications can be received over a network would lead one of ordinary skill in the art to the step of transferring the TPM identity, the non-migratable key and a certificate from a certifying authority to a credit card company.

We find that combining the method of creating a TPM identity in TCPA with the knowledge that credit card applications can be received over a network does not lead one of ordinary skill in the art to the claimed methods and systems of claims 7, 21, 26, and 27. A prima facie case of obviousness under 35 U.S.C. § 103(a) has therefore not been established, and we reverse the rejections of claims 7, 21, 26, and 27 and their dependent claims 8-12 and 22-24.

As further explained below, we will enter a new ground of rejection on claims 13-15 under 35 U.S.C. § 112, second paragraph, on the ground that claims 13-15 are indefinite. Therefore, the prior art rejection must fall because they are necessarily based on speculative assumption as to the meaning of the claim. *See In re Steele*, 305 F.2d 859, 862-63 (CCPA 1962).

NEW GROUND OF REJECTION

Pursuant to 37 C.F.R. § 41.50(b) (2007) a new grounds of rejection is included in this opinion.

Claim 13 recites "wherein the creating step further comprises creating a public/private key pair." Claim 13 depends on claim 7. Claim 7 recites two creating steps: 1) creating a TPM identity and 2) creating, at the customer's computer system, a non-migratable key. It is unclear whether the step of creating the TPM identity or the step of creating the non-migratable key further comprises creating a public/private key pair. Claim 14 depends on claim 13 and also recites "the public/private key pair" created in claim 13.

Claim 15 depends directly on claim 14 and indirectly on claims 7 and 13. Claim 15 recites "the step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system further comprises …." However, none of claims 7, 13, or 14 recite a step of transferring the public/private key pair and the second certificate from the second server supporting the credit card company to the customer's computer system. Further, claims 7, 13, or 14 do not recite a second certificate.

Although antecedent basis can be present by implication (*see Slimfold Mfg. Co. v. Kinkead Indus., Inc.*, 810 F.2d 1113, 1116 (Fed. Cir. 1987), where the lack of antecedent basis causes a claim to be insolubly ambiguous, it is proper to reject the claim under § 112, 2nd ¶, thus requiring applicant to more precisely define the invention. ("Lack of an antecedent basis in a claim could render it invalid under 35 U.S.C. § 112," *In re Altenpohl*, 500 F.2d 1151, 1156 (CCPA 1974).) "It is the applicant['s] burden to precisely define the invention, not the PTO's." *In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997); *see also* 35 U.S.C. § 112 ¶ 2 ("The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.").

> The second paragraph of 35 U.S.C. § 112 requires that the specification of every patent must "conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." This requirement serves a public notice function, ensuring that the patent specification adequately notifies the public of the scope of the patentee's right to exclude. *See Honeywell Int'l, Inc. v. Int'l Trade Comm'n,* 341 F.3d 1332, 1338 (Fed. Cir. 2003). A claim satisfies the definiteness requirement of § 112 "[i]f one skilled in the art would understand the bounds of the claim when read in light of the specification." *Exxon Research & Eng'g Co. v. United States,* 265 F.3d 1371, 1375 (Fed. Cir. 2001). A claim will be found indefinite only if it

> "is insolubly ambiguous, and no narrowing construction can properly be adopted...." *Id.*

Praxair, Inc. v. ATMI, Inc., 543 F.3d 1306, 1319 (Fed. Cir. 2008). We find that these claims are insolubly ambiguous.

Therefore, claims 13-15 are rejected under 35 U.S.C. § 112, 2nd paragraph, for failing to particularly point out and distinctly claim the subject matter which the Appellant regards as the invention.

CONCLUSIONS OF LAW

We conclude that the Appellant has shown that the Examiner erred in rejecting claims 1-27 under 35 U.S.C § 103(a) as unpatentable over TCPA.

A new ground of rejection has been applied to claims 13-15 under 35 U.S.C. § 112, second paragraph.

DECISION

The decision of the Examiner to reject claims 1-27 is reversed.

We enter a new ground of rejection of claims 13-15 under 35 U.S.C. § 112, second paragraph.

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b) (effective September 13, 2004, 69 Fed. Reg. 49960 (August 12, 2004), 1286 Off. Gaz. Pat. Office 21 (September 7, 2004)). 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that the Appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> • (1) Reopen prosecution. Submit an appropriate amendment of the claims so rejected or new evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the proceeding will be remanded to the examiner . . . .
>
> • (2) Request rehearing. Request that the proceeding be reheard under § 41.52 by the Board upon the same record . . . .

REVERSED; 37 C.F.R. § 41.50(b)

hh

Robert A. Voigt, Jr.
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201